

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 168 137 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.01.2002 Bulletin 2002/01

(51) Int Cl.7: G06F 1/00, G06K 7/00,
G11B 20/00

(21) Application number: 01112947.5

(22) Date of filing: 06.06.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR

Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 23.06.2000 IT MI001425

(71) Applicant: IPM-NET S.p.A.
80022 Arzano (Prov. of Napoli) (IT)

(72) Inventor: Della Valle, Stefano
20043 Arcore (IT)

(74) Representative: Modiano, Guido, Dr.-Ing. et al
Modiano & Associati SpA Via Meravigli, 16
20123 Milano (IT)

(54) Smart card reader with usb interface for connection to personal computers and the like

(57) A smart card reader (1) suitable to be connected to a personal computer, comprising at least one connector (3) adapted to be connected to a communication port of the computer and at least one smart card which,

when activated, is suitable to enable a communication between the reader (1) and the personal computer, in order to allow a user to access an application program installed on the personal computer.

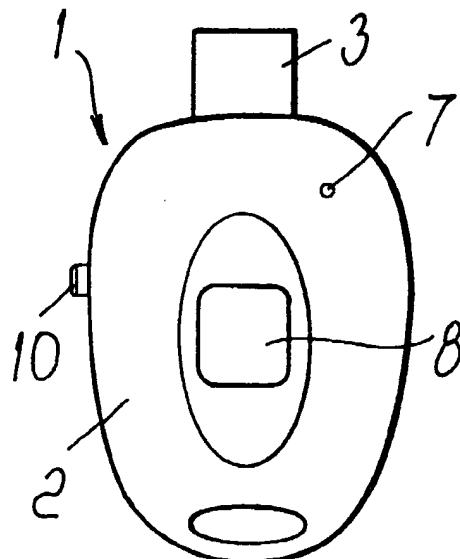


Fig. 1

EP 1 168 137 A1

Description

[0001] The present invention relates to a smart card reader with USB interface, for connection to personal computers and the like.

[0002] It is known that software houses need to copy-protect their programs, which require hundreds of man-hours to be developed.

[0003] Illegal copying of programs is one of the factors that leads to extremely high costs for software. Accordingly, it seems absolutely necessary for software houses to find a system which allows them to avoid fraudulent duplication of said programs.

[0004] Currently, one of the most widely used systems consists in providing electronic keys which are generally connected to the parallel port of the computer; without said keys, the software program does not run.

[0005] Such electronic keys are hardware components dedicated expressly to an appropriately provided computer and/or program, since they have wiring which corresponds to the hardware structure of the computer proper and to software control functions.

[0006] Accordingly, one of the drawbacks suffered by hardware keys thus conceived is that they are expressly dedicated to a single computer, so that they cannot be used on different computers and cannot be reprogrammed in any way.

[0007] Another drawback of conventional electronic keys is that an expert in the field can duplicate the hardware configuration of the electronic key and therefore bypass the protection devised by the software house for its program.

[0008] Moreover, conventional electronic keys cannot be personalized by the user; it is therefore impossible to determine unequivocally whether the user who is using the key is the one who is authorized to do so.

[0009] Accordingly, for example if the electronic key is lost, anyone can use a given program already installed on a personal computer, with the dedicated key.

[0010] This of course entails a fault in data security, since the user has no assurance that his program cannot be run in any way by unauthorized individuals, since operation is entrusted exclusively to the electronic key, which if lost can be used by anyone on the personal computer on which said program is installed.

[0011] The aim of the present invention is to provide a smart card reader with USB interface which allows to connect to the personal computer an electronic key for enabling the operation of a given software program or of the entire personal computer and in which the smart card is able to interact with the control application or software installed on the computer.

[0012] Within this aim, an object of the present invention is to provide a smart card reader with USB interface for connection to a personal computer which is provided with means for unequivocal identification of the user, capable of enabling the operation of a given software application or of the entire system only if the user who is

using the smart card reader is the one who is actually authorized to do so.

[0013] Another object of the present invention is to provide a smart card reader which allows to use the same reader on different personal computers without the need to install appropriate software.

[0014] Another object of the present invention is to provide a smart card reader for connection to a personal computer and the like which is highly reliable, and be relatively simple to manufacture and at competitive costs.

[0015] This aim and these and other objects which will become better apparent hereinafter are achieved by a smart card reader suitable for connection to a personal computer, characterized in that it comprises at least one connector adapted to be connected to a communication port of said computer and at least one smart card which, when activated, is suitable to enable a communication between the reader and the personal computer, in order to allow a user to access an application program installed on such personal computer.

[0016] Further characteristics and advantages of the present invention will become better apparent from the description of preferred but not exclusive embodiments of the smart card reader according to the present invention, illustrated only by way of non-limitative example in the accompanying drawings, wherein:

Figure 1 is a top plan view of the card reader according to the present invention;

Figure 2 is a side view of the device of Figure 1; Figure 3 is a bottom plan view of the card reader according to the present invention; and

Figure 4 is a block diagram of the card reader according to the present invention.

[0017] With reference to the figures, the smart card reader according to the present invention, generally designated by the reference numeral 1, comprises an external container 2 which has, in a protruding position,

40 a connector 3, preferably of the USB type, for connection to a standard port of a personal computer or the like. [0018] The body 2 has, in an upward region and below the connector 3, at least one slot 4 which allows to insert a smart card 5 in which the application program for communication with the personal computer is stored.

[0019] Conveniently, the container 2 can be provided, in a downward region, with a window 6 which allows to view the smart card 5 inserted in the slot 4.

[0020] Preferably, the smart card can be of the SIM (Subscriber Identity Module) type.

[0021] Moreover, the smart card reader 1 is preferably provided with at least one LED 7 which is suitable to indicate to the user that a correct connection is present, by means of the USB connector 3, between the reader 1 and the personal computer.

[0022] Access to the personal computer or to an application running on the personal computer is enabled

by the smart card 5 without further interaction by the user or, if provided by the system, by entering a PIN (Personal Identification Number) by means of the keyboard of the personal computer.

[0023] Accordingly, in this first embodiment of the reader according to the invention, the smart card 5 allows to perform an advanced interaction with the software application installed on the personal computer. In particular, a portion of the application program installed on the personal computer can be stored on the smart card, so that if the reader 1 is not present the program that is present on the personal computer is completely unusable because part of it is missing.

[0024] A second embodiment of the reader according to the present invention provides, instead of entering the PIN to enable the smart card, or alternatively in addition thereto, an internal enabling function by direct identification of the user by the reader 1.

[0025] For this purpose sensor means 8 are provided, which are arranged for example at the upper face of the container 1, by which it is possible to detect the print of one of the user's fingers, for example the thumb.

[0026] Figure 4 illustrates, as a block diagram, a possible implementation of the reader according to the present invention.

[0027] In this block diagram, the sensor means 8 is connected to microprocessor means 9, which are in turn connected to memory means 10. In this case, the memory means 10 contain the user's fingerprint, which is compared in each instance, by the microprocessor means 9, with the print left by the user on the sensor means 8 by resting his finger on said sensor means.

[0028] Accordingly, access to the smart card is enabled, in this manner, thanks to a method which allows to ensure the inviolability of the system.

[0029] In fact it is known that fingerprints cannot be duplicated and therefore recognition of the user's fingerprint by the sensor means 8 gives the user the assurance that the reader cannot be used fraudulently.

[0030] In this case, therefore, it would be possible to avoid the need to memorize a PIN and enter it each time in order to access the functions of the smart card 5.

[0031] Since the information (data) related to the fingerprints of the owner of the reader 1 are stored in the reader itself, and more specifically in the memory means 10, they cannot be accessed in any way.

[0032] Since security is ensured by elements which are all contained in the reader according to the invention, it can be transferred from one personal computer to another and used by a same user regardless of the workstation, without the need to install appropriate software for each different key on each specific personal computer.

[0033] A third embodiment of the smart card reader according to the present invention provides for the addition of application or identification selection means 11 which, by being moved to different positions, allow to enable a corresponding number of PINs.

5 [0034] The application selection means 11 are associated with the sensor means 8; therefore, once the user's fingerprint has been recognized, the PIN that corresponds to the position indicated by the selection means 11 is sent to the smart card 5.

10 [0035] This allows to use different smart cards 5, each with its own specific PIN, or a multiple-application smart card, in which each application has a separate PIN which can be selected by the selection means 11.

15 [0036] The selection means 11 are operatively connected to the microprocessor means 9, as already shown in Figure 4; such means are in turn connected to an internal bus 12, which connects the microprocessor means 9 to the sensor means 8, to the memory means 10 and to second microprocessor means 13, which control the connection means 3 which allow the connection of the reader 1 to the USB serial port of a personal computer 15.

20 [0037] The reference numeral 5 (Figure 4) illustrates, like in the preceding figures, the smart card, inserted in a smart card reader, which is designated by the reference numeral 16 and is accommodated in the container 2 and connected to a driver 17 of the smart card 5, being in turn connected to the internal bus 12 of the reader.

25 [0038] The second microprocessor means 13 are adapted to handle communication toward the personal computer 15, while the smart card 5 has an additional microprocessor, schematically designated by the reference numeral 18 for the sake of simplicity, which is adapted to interface the first and second microprocessor means 9 and 13 with the smart card 5.

30 [0039] With reference to the above cited figures, the operation of the reader according to the invention is as follows.

35 [0040] First of all, an initialization step is performed; during this step, after connecting the reader 1 to the USB serial port of the computer 15, by means of the USB connector 3, an appropriate software program interacts with the microprocessor means 9, which compare the fingerprint stored in the memory means 10 with the print of the finger detected by the sensor means 8.

40 [0041] At this point, the software program activates a function for processing the fingerprint by means of the first microprocessor means 9, and if the quality of the detected fingerprint is sufficient, the first microprocessor means 9 send a confirmation message to the software program.

45 [0042] The significant features of the fingerprint are encrypted and stored in the memory means 10.

50 [0043] Finally, the software program communicates a PIN code of the associated smart card 5. The PIN is encrypted and stored.

55 [0044] The PIN for enabling the smart card 5 can be sent, as mentioned, either by manually entering it or by providing for the automatic sending of the PIN by the first microprocessor means 9, after the user's fingerprint has been recognized by the sensor means 8.

[0045] In this case, the smart card replies to the un-

lock request exactly as if the PIN had been entered by means of the keyboard of the personal computer 15.

[0046] If the selection means 11 are present, at this point it is possible to select, in each instance, the sending of a chosen PIN, selected by the selection means 11.

[0047] In practice it has been observed that the smart card reader according to the invention fully achieves the intended aim and objects, since it allows to provide an electronic security key for a software program and allows, by using a smart card inside it, to store for example part of the program on the smart card itself, to send a smart card activation recognition PIN which accordingly enables communication with the personal computer to which the reader is connected, and to detect an unequivocal distinctive feature of the user, such as his fingerprint, in order to allow him to access the software program installed on the personal computer.

[0048] Finally, the possibility of having a smart card in which multiple PINs are stored allows the user, by way of the selection means, to select in each instance the PIN he wants and therefore for example to allow the enabling of a particular software program or to differentiate the user, for example by storing the fingerprints of multiple users on the same reader.

[0049] In this manner, the reader according to the invention can be used not only on different personal computers but also for different software programs, allowing to program in each instance the chosen PIN in order to allow communication between the reader and the personal computer, as regards a particular software program to which the user is to be allowed access.

[0050] The reader thus conceived is susceptible of numerous modifications and variations, all of which are within the scope of the same inventive concept; all the details may furthermore be replaced with other technically equivalent elements.

[0051] In practice, the materials used, as well as the contingent shapes and dimensions, so long as they are compatible with the specific use, may be any according to requirements and to the state of the art.

[0052] The disclosures in Italian Patent Application No. MI2000A001425 from which this application claims priority are incorporated herein by reference.

[0053] Where technical features mentioned in any claim are followed by reference signs, those reference signs have been included for the sole purpose of increasing the intelligibility of the claims and accordingly, such reference signs do not have any limiting effect on the interpretation of each element identified by way of example by such reference signs.

Claims

1. A smart card reader suitable for connection to a personal computer, characterized in that it comprises at least one connector meant to be connected to a communication port of said computer and at least

one smart card which, when activated, is suitable to enable a communication between said reader and said personal computer, in order to allow a user to access an application program installed on said personal computer.

- 5 2. The reader according to claim 1, characterized in that said connector of said reader is a USB connector, and in that said communication port of said personal computer is a USB serial communications port.
- 10 3. The reader according to claim 1, characterized in that it comprises a container which is suitable to accommodate said at least one smart card, a slot being formed in said container for the insertion of said at least one smart card.
- 15 4. The reader according to one or more of the preceding claims, characterized in that said container comprises a window which is arranged so as to allow to view said smart card when said smart card is inserted in said slot of the container.
- 20 5. The reader according to one or more of the preceding claims, characterized in that it comprises first microprocessor means which are connected to memory means and are connected, by way of an internal bus, to second microprocessor means which are suitable to handle the communication between said reader and said personal computer.
- 25 6. The reader according to one or more of the preceding claims, characterized in that it comprises sensor means which are arranged at the surface of said container and are connected to said first microprocessor means.
- 30 7. The reader according to claim 6, characterized in that said sensor means comprise at least one fingerprint sensor which is suitable to detect the fingerprint of a user and compare it, through said memory means and said first microprocessor means, with a fingerprint which is stored beforehand in said memory means and unequivocally identifies the authorized user.
- 35 8. The reader according to one or more of the preceding claims, characterized in that it comprises selection means which are connected to said first microprocessor means and are suitable to select a specific PIN of said at least one smart card.
- 40 9. The reader according to one or more of the preceding claims, characterized in that said at least one smart card contains part of said software program installed on said personal computer.
- 45 55

10. The reader according to one or more of the preceding claims, characterized in that it comprises at least one LED which is suitable to give indications as to the result of the connection between said reader and said personal computer. 5

10

15

20

25

30

35

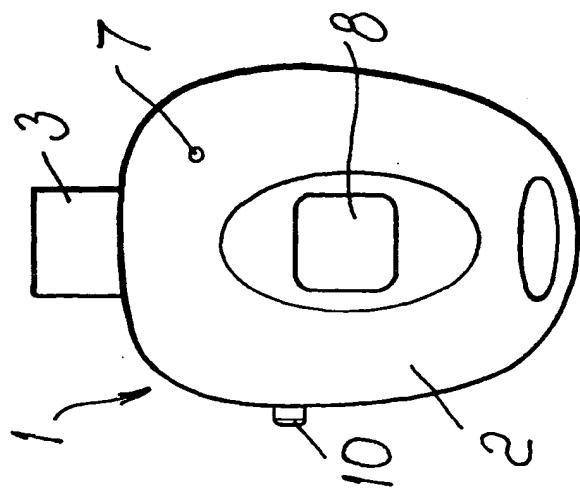
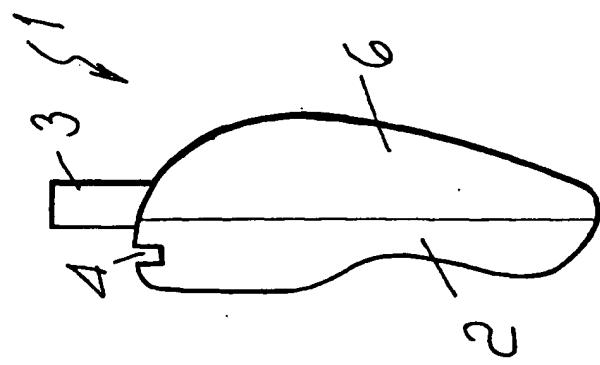
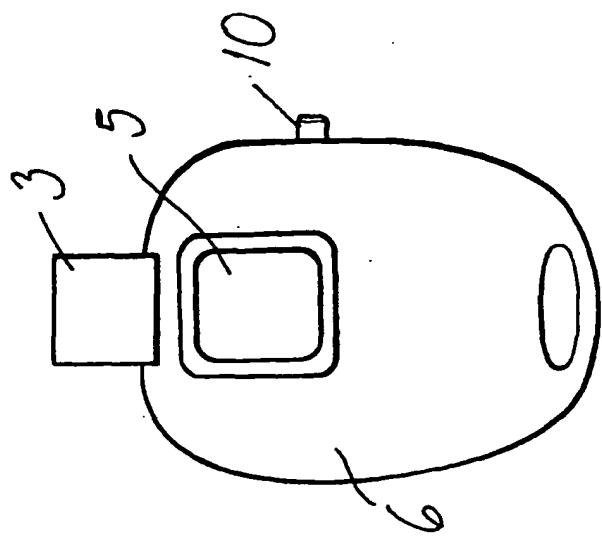
40

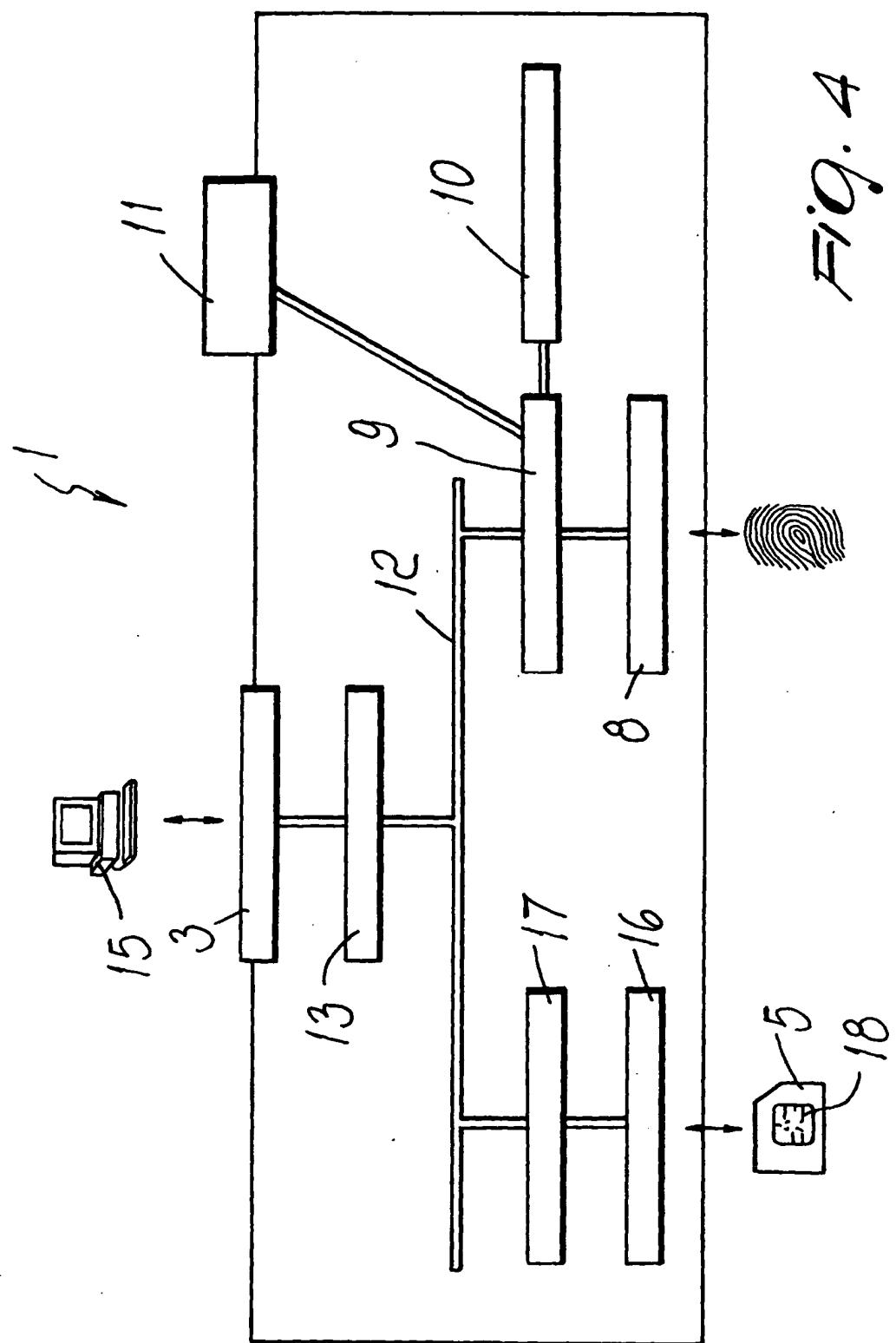
45

50

55

5







European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 11 2947

DOCUMENTS CONSIDERED TO BE RELEVANT			CLASSIFICATION OF THE APPLICATION (Int.Cl.)
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	
Y	WO 00 23936 A (LITRONIC INC) 27 April 2000 (2000-04-27) * page 1, line 1 - page 17, line 6 * * abstract; figures 1,2A *	1-10	G06F1/00 G06K7/00 G11B20/00
Y	US 4 757 534 A (MATYAS STEPHEN M ET AL) 12 July 1988 (1988-07-12) * abstract * * column 8, line 23 - line 30 *	1-10	
Y	EP 0 843 250 A (ALPS ELECTRIC IRELAND LTD) 20 May 1998 (1998-05-20) * abstract; figures 1,2,5 *	1-10	
Y	EP 0 881 557 A (SIEMENS AG) 2 December 1998 (1998-12-02) * column 1, line 5 - line 22 * * column 14, line 5 - line 13 *	1-10	
Y	US 5 131 091 A (MIZUTA MASAHIRO) 14 July 1992 (1992-07-14) * abstract * * column 1, line 11 - line 51 * * column 5, line 2 - line 3 *	1-10	TECHNICAL FIELDS SEARCHED (Int.Cl.) G06F G06K G11B
The present search report has been drawn up for all claims			
Place of search	Date of completion of the search	Examiner	
MUNICH	30 August 2001	Heusler, N	
CATEGORY OF CITED DOCUMENTS		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : Intermediate document			

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 01 11 2947

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-08-2001

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0023936	A	27-04-2000	US	6168077 B	02-01-2001
			AU	6268699 A	08-05-2000
			US	2001000405 A	26-04-2001
US 4757534	A	12-07-1988	CA	1238427 A	21-06-1988
			DE	3587072 A	18-03-1993
			DE	3587072 T	12-08-1993
			EP	0191162 A	20-08-1986
			JP	1630801 C	26-12-1991
			JP	2060007 B	14-12-1990
			JP	61145642 A	03-07-1986
EP 0843250	A	20-05-1998	IE	960815 A	19-11-1997
			US	6056193 A	02-05-2000
EP 0881557	A	02-12-1998	NONE		
US 5131091	A	14-07-1992	JP	1296361 A	29-11-1989